Newsletter Datenschutz

konzept 17

Ihr Datenschutz-Info Blatt für mehr Sicherheit in Ihrem Unternehmen

Liebe Leserin, lieber Leser,

manchmal ist es anders, als man denkt oder bisher gehört hat. Dafür liefert unsere aktuelle Ausgabe gleich mehrere Beispiele.
Da wäre zum einen die Pflicht, Hackerangriffe, von denen personenbezogene Daten betroffen sind, zu melden. Reicht eine Meldung an die Polizei aus, oder ist diese Meldung gar nicht vorgeschrieben? Der erste Beitrag klärt darüber auf.

Oder wie ist es mit Datenpannen beim Versand von Informationen mit Personenbezug? Passiert so etwas nur per E-Mail, oder sind auch klassische Briefe und Pakete betroffen? Auch hier erfahren Sie, wie es tatsächlich ist.
Zwei weitere Beispiele, die anders sind, als man vermuten könnte: So gibt es gegenwärtig viele Berichte über Unsicherheiten bei Datentransfers in die USA. Was steckt dahinter?

Der vierte Beitrag wirft ein neues Licht auf das scheinbar bekannte Thema Online-Tracking. Wie Sie erfahren werden, können selbst Kartendienste, die innerhalb von Webseiten eingebunden sind, zur Nachverfolgung Ihrer Online-Aktivitäten führen.

Ihr Frank Berns, Datenschutzbeauftragter

Impressum
Redaktion: Frank Berns,
Datenschutzbeauftragter, Geschäftsführer

Anschrift:
Konzept 17 GmbH
Westring 3
24850 Schuby
Amtsgericht Flensburg: HRB 12329
Telefon: 0049 4621 5 30 40 50
E-Mail: mail@konzept17.de

Strafanzeige nach Hackerangriff? Wer informiert werden muss

8 von 10 Unternehmen in Deutschland waren bereits von Datendiebstahl, Spionage oder Sabotage betroffen, berichtet der Digitalverband Bitkom. Doch wie reagiert man, wenn ein Cyberangriff auf das eigene Unternehmen festgestellt wird?

Die Cyberattacke kommt

Wenn 80 Prozent der Betriebe in Deutschland bereits einem Angriff durch Hacker und andere Internetkriminelle zum Opfer gefallen sind, hofft man, zu den anderen 20 Prozent zu gehören. Doch IT-Sicherheitsfachkräfte warnen: Es ist nicht mehr die Frage, ob man angegriffen wird, sondern nur noch, wann.

Zudem geht man in der IT-Sicherheit von einer hohen Dunkelziffer aus – so manches Unternehmen, das scheinbar noch nicht attackiert wurde, hat dies bisher nur noch nicht entdeckt. Viele Cyberangriffe bleiben lange unerkannt – für Tage, Wochen oder Monate.

Cyberattacken zu erkennen ist nur der erste Schritt

Deshalb versuchen viele Unternehmen, darin besser zu werden einen Hackerangriff erkennen zu können, und zwar deutlich schneller als bisher. Doch allein das Erkennen eines Cyberangriffs reicht nicht aus. Um die Folgeschäden so klein wie möglich zu halten, müssen Gegenmaßnahmen eingeleitet werden.
Dazu gehört es auch, alle relevanten Stellen über den entdeckten Cyberangriff zu informieren. Doch wer muss eigentlich alles informiert werden? Ist es bei einem Einbruch in die IT-Systeme ähnlich wie bei einem Einbruch in ein Gebäude? Ruft man also die Polizei an?

Meldepflichten gibt es mehrere

In den vergangenen Jahren ist viel darüber berichtet worden, dass entdeckte Cyberangriffe an den Datenschutzbeauftragten bzw. die Datenschutzbeauftragte gemeldet werden sollen, denn viele Attacken auf die IT-Systeme betreffen auch personenbezogene Daten, etwa von Beschäftigten, Kunden oder Lieferanten.
Tatsächlich sieht das Datenschutzrecht, die Datenschutz-Grundverordnung (DSGVO), auch Meldepflichten vor, sowohl an die zuständige Aufsichtsbehörde für den Datenschutz als auch in bestimmten Fällen an die Betroffenen selbst – also die Personen, deren Daten betroffen sind.
Doch das ist nicht alles: Neben der Meldepflicht nach der DSGVO können weitere Mitteilungspflichten bestehen. So müssen zum Beispiel Sozialleistungsträger eine Verletzung des Schutzes von Sozialdaten auch der zuständigen Rechts- oder Fachaufsichtsbehörde melden. Betreiber kritischer Infrastrukturen, von Energieversorgungsnetzen und

von bestimmten Energieanlagen haben eine Pflicht zur Meldung an das Bundesamt für Sicherheit in der Informationstechnik (BSI), wenn bestimmte Störungen auftreten – wie kürzlich eine Datenschutzaufsichtsbehörde klarstellte. Doch was ist eigentlich mit der Meldung an die Polizei?

Rechte und Pflichten

„Es besteht grundsätzlich keine gesetzliche Verpflichtung, nach der DSGVO meldepflichtige Vorfälle auch den Strafverfolgungsbehörden mitzuteilen. Dies führt in der Praxis nicht selten dazu, dass eine Strafanzeige unterbleibt", berichtet etwa zum Beispiel der Bayerische Landesbeauftragte für den Datenschutz. Doch eine Strafanzeige kann sehr sinnvoll sein und zur Aufklärung und zur Verhinderung weiterer Schäden beitragen. Die Strafanzeige kann Ermittlungen einleiten, die darauf abzielen, die Hintergründe und Ursachen des Angriffs zu analysieren, so der Landesdatenschutzbeauftragte.
Durch die Zusammenarbeit mit den Ermittlungsbehörden können wichtige Informationen über den Angriff erlangt werden – etwa über die Angreifer und mögliche Schwachstellen in den eigenen Systemen. Dieses Wissen kann einem Unternehmen dabei helfen, die direkten Auswirkungen eines Hackervorfalls zu begrenzen und zukünftige Angriffe besser zu verhindern. Deshalb sollte bei einer Cyberattacke immer auch die Möglichkeit geprüft werden, die Polizei einzuschalten. Das sollte aber nicht dazu führen, eine Datenpanne durch Hackerangriffe nicht mehr an die zuständige Datenschutzaufsichtsbehörde zu melden. Die eine Meldung ersetzt die andere Meldung nicht.

Wenn Sie unsicher sind, an wen Sie den Verdacht melden sollen, dass es einen Hackerangriff auf die IT-Systeme des Unternehmens gegeben haben könnte, wenden Sie sich an Ihre Datenschutzbeauftragte bzw. Ihren Datenschutzbeauftragten. Helfen Sie dabei, die Dunkelziffer bei Cyberattacken so klein wie möglich zu machen!

Pannen beim klassischen Postversand

Privat schreiben viele Menschen keine Briefe mehr. Stattdessen nutzen sie die Möglichkeiten der sozialen Netzwerke. Kein Wunder, dass es dann zu Datenschutzvorfällen kommt, wenn in der Arbeit doch einmal der gute alte Brief genutzt werden muss.

Für viele sind Briefe etwas Antikes

Man muss nur einmal die neuen Azubis fragen, wie oft sie in ihrem Leben schon selbst einen Brief geschrieben haben. Viele müssen auf diese Frage völlig passen. Manche erinnern sich zumindest an einige wenige Briefe. Kein Wunder, dass manche Postfilialen schon Muster dafür aushängen, wie man einen Briefumschlag richtig beschriftet, wohin also dort die Anschrift des Empfängers gehört, wohin die Anschrift des Absenders und wo der richtige Platz für die Briefmarke ist. Darüber kann man schmunzeln. Doch bildet diese Situation eine schwierige Ausgangslage, wenn es um das Vermeiden von Datenpannen beim Briefversand geht.

Das sind „Pannen-Klassiker" der Aufsichtsbehörden

Datenschutzvorfälle müssen bekanntlich in aller Regel der zuständigen Aufsichtsbehörde für den Datenschutz gemeldet werden.

In den Berichten der Aufsichtsbehörden schlägt sich das beschriebene Unwissen in Bezug auf Briefe deutlich nieder. Wer schon nicht weiß, wie man einen Briefumschlag richtig zu beschriften hat, achtet umso weniger auf andere Tücken. Hier die wichtigsten „Pannen-Klassiker:

- Auf dem Umschlag steht schlicht der falsche Adressat, den der Inhalt nichts angeht.
- Es werden neben den richtigen Unterlagen noch Dokumente mit eingetütet, die ganz andere Personen betreffen.
- Fensterumschläge erlauben unzulässige Einblicke in den Inhalt des Briefes.
- Fehlerhaft arbeitende Kuvertiermaschinen verschließen einzelne Briefumschläge gar nicht oder nur teilweise.

Wichtig sind genaue Vorgaben und das Üben

Gerade weil die Rolle des Briefversands deutlich kleiner geworden ist, sind genaue Vorgaben nötig. Denn was seltener vorkommt, funktioniert umso häufiger nicht. Außerdem ist in diesem Zusammenhang wichtig: üben, üben, üben! Bei neuen Mitarbeiterinnen und Mitarbeitern – also nicht nur bei Azubis! – ist stets damit zu rechnen, dass sie weder privat noch in ihren bisherigen beruflichen Tätigkeiten Briefe versenden mussten. Deshalb

muss man klären, ob sie wissen, wie es geht. Ansonsten brauchen sie eine Einweisung und müssen Gelegenheit erhalten, das Ganze auch einmal unter Begleitung zu machen.

Die Versender sind ein Sonderproblem

Wenig ändern lässt sich an der Zuverlässigkeit der Postdienstleister. Viele behaupten, sie hätten sich in den letzten Jahren verschlechtert. Die statistischen Daten dazu, etwa der zuständigen staatlichen Aufsichtsbehörden, sprechen keine eindeutige Sprache. Datenschutzbehörden berichten allerdings mit erkennbarer Verwunderung vermehrt davon, dass vereinzelt sogar Postsendungen erheblichen Umfangs und Gewichts auf dem Postweg verloren gehen.

Umso wichtiger ist die Nachverfolgbarkeit

Wenn ein Brief nicht ankommt, den man verschickt hat, kann man beim Postdienstleister einen sogenannten „Nachforschungsantrag“ stellen. Die Fälle, in denen der Brief dann dadurch gefunden wird, sind allerdings äußerst selten. Umso größere Bedeutung erlangen die Versendungsformen, bei denen eine Nachverfolgung der Sendung möglich ist. Dies setzt voraus, dass die Postsendung (also Brief oder Paket) auf ihrem Weg immer wieder an bestimmten Knotenpunkten registriert wird. Dann lässt sich ihr Weg rekonstruieren. Die Chance, einen Verlust auf dem Postweg aufzuklären, wächst dadurch erheblich.

Dafür gibt es besondere Versendungsformen

Für Briefe gibt es die zusätzliche Dienstleistung „Einwurfeinschreiben“. Bei ihr dokumentiert die Zustellkraft den Einwurf des Briefs in den Briefkasten des Empfängers mit Datum und Uhrzeit. Kommt es zu Streitigkeiten darüber, ob die Zustellung erfolgt ist, steht die Zustellkraft als Zeuge zur Verfügung. Allerdings kostet ein Einwurfeinschreiben ein erhebliches Extraporto. Bei Paketen ist die Möglichkeit der Nachverfolgung automatisch ein Teil der bezahlten Dienstleistung – muss also nicht extra gebucht werden.

Der Versand von USB-Sticks verlangt besondere Sorgfalt

In manchen Lebensbereichen, etwa im Gesundheitswesen, kommt der Versand von USB-Sticks noch häufig vor. Dabei kommt es schnell vor, dass beim Transport der Stick den Umschlag durchbohrt, dann herausrutscht und verloren geht. Diese Gefahr gilt es zu bannen. Geeignetes Instrument hierfür sind beispielsweise Luftpolsterumschläge. Außerdem ist es angezeigt, die Dateien auf dem Stick zu verschlüsseln. Selbst wenn er dann verloren geht, kann niemand die Daten lesen.

Datentransfer in die USA

Manchmal herrscht Aufregung, obwohl dazu akut kein Anlass besteht. Funktionieren die Dinge bei der Übermittlung personenbezogener Daten in die USA auf der Basis des „Angemessenheitsbeschlusses“ für die USA, kann auf absehbare Zeit davon ausgegangen werden, dass hier alles problemlos weiterlaufen kann wie bisher.

Die USA haben eine besondere Stellung

Die USA sind auf zahlreichen Gebieten der IT unverändert Weltmarktführer. Fast alle nutzen Produkte von Unternehmen wie Google und Microsoft. Hinzu kommt spezifische Branchen-Software, die nur in den USA erhältlich ist. Besonders die Anwendung von webbasierten Systemen setzt oft zwingend den Transfer von Daten in die USA voraus. Hierfür ist eine Rechtsgrundlage erforderlich.

Der Datenschutzrahmen EU-USA hat eine besondere Rolle

An dieser Stelle kommt der „Datenschutzrahmen EU-USA“ ins Spiel. Dabei handelt es sich um eine Vereinbarung zwischen der EU und den USA. Unternehmen in den USA können sich den Bedingungen dieser Vereinbarung unterwerfen und gelten dann als Datenempfänger, bei denen ein angemessenes Datenschutzniveau herrscht. Personenbezogene Daten können an sie unter denselben Bedingungen transferiert werden, wie sie sonst nur für Datenempfänger innerhalb der EU gelten.

Die Rolle der EU-Kommission ist dabei zentral

Möglich geworden ist das, weil die EU-Kommission einen „Angemessenheitsbeschluss“ gemäß Art. 45 DSGVO gefasst hat. Mit ihm hat die EU-Kommission verbindlich festgestellt: Bei Datenempfängern in den USA, die sich dem Datenschutzrahmen „EU-USA““ unterworfen haben, besteht ein angemessenes Datenschutzniveau. Datenübermittlungen an sie sind deshalb ohne besondere Genehmigung zulässig.

Bisher läuft alles gut

Das geschilderte Verfahren läuft problemlos seit dem 10.07.2023, dem Tag der Anwendbarkeit des Angemessenheitsbeschlusses. Zwar wird seine Rechtmäßigkeit immer wieder einmal infrage gestellt. Aber derzeit ist beim Europäischen

Gerichtshof (EuGH) kein Verfahren anhängig, das seine Rechtmäßigkeit verneinen könnte. Ein französischer Europaabgeordneter hat zwar versucht, seine Anwendung durch eine einstweilige Anordnung des EuGH stoppen zu lassen, doch hat der EuGH diesen Antrag zurückgewiesen.

Es gibt ungute Erinnerungen an den EuGH

Die beiden Vorgänger des „Datenschutzrahmens EU-USA" fanden beim EuGH allerdings keine Gnade. Viele werden sich noch an die Stichworte „Safe Harbor" und „Privacy Shield" erinnern. Dabei handelte es sich ebenfalls um Abkommen zu Übermittlung personenbezogener Daten in die USA, für welche die EU-Kommission einen Angemessenheitsbeschluss gefasst hatte. Beide Angemessenheitsbeschlüsse erklärte der EuGH für nichtig. Doch kann er – wie alle Gerichte – nicht von sich aushandeln, sondern nur, wenn es entsprechende Klagen oder Anträge gibt. Und das ist derzeit eben nicht der Fall.

Trump sorgt auch hier für Unruhe

Dass Maßnahmen des US-Präsidenten Trump Unruhe auslösen, gehört inzwischen in vielen Lebensgebieten zum Alltag. Auch hinsichtlich des Angemessenheitsbeschlusses für Datentransfers in die USA ist es ihm gelungen, für Unruhe zu sorgen. Im Angemessenheitsbeschluss sind mehrere unabhängige US-Regierungsbehörden erwähnt, die bei möglichen Beschwerden von betroffenen Personen eine teils wichtige Funktion haben. Sie müssen deshalb handlungsfähig sein. Das ist derzeit schwierig, weil Präsident Trump bei einigen dieser Behörden führende Repräsentanten abberufen hat, ohne sie zu ersetzen. Ob dies im Ernstfall, also beim Eingang von Beschwerden betroffener Personen, tatsächlich zu Problemen führt, ist derzeit aber noch unklar.

Von allein kann nichts geschehen

Umso wichtiger erscheint folgender Hinweis: Egal, was Präsident Trump noch veranlassen sollte, es führt auf keinen Fall dazu, dass der Angemessenheitsbeschluss der EU-Kommission automatisch außer Kraft tritt. Da beim EuGH kein entsprechendes Verfahren anhängig ist, könnte der Angemessenheitsbeschluss nur durch einen Aufhebungsbeschluss der EU-Kommission aus der Welt geschafft werden. Auch dies würde aber auf keinen Fall über Nacht geschehen. Vielmehr wären Verfahrensabläufe einzuhalten, die öffentliche Aufmerksamkeit erfahren würden.

Bewahren Sie einfach Ruhe

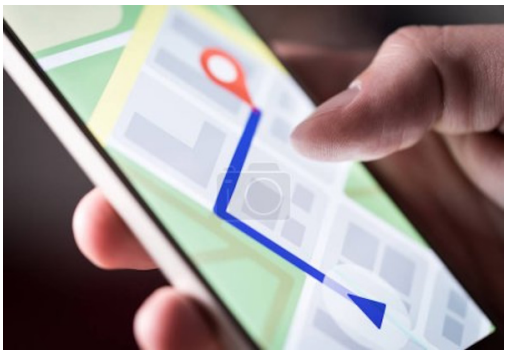
Für den Datenschutzalltag gilt daher: Verwenden Sie Ihre wertvolle Zeit nicht darauf, theoretische Diskussionen zu verfolgen. Wenden Sie bei Datenübermittlungen in die USA vielmehr die vorhandenen Regelungen weiterhin wie gewohnt an. Das gilt besonders auch für den Angemessenheitsbeschluss zum „Datenschutzrahmen EU-USA".

Online-Tracking: Was Sie als Besucher von Webseiten wissen sollten

Viele Webseiten binden Kartendienste wie Google Maps oder Videos von YouTube ein. Was nützlich und informativ erscheint, kann zu einem ungewollten Nachverfolgen Ihrer Online-Aktivitäten führen.

Wo ist die Filiale eigentlich? Und wo kann ich parken?

Stellen Sie sich vor, Sie werden



gebeten, eine Lieferung für Ihre Abteilung abzuholen. Das Fachgeschäft, bei dem bestellt wurde, ist Ihnen nicht bekannt. Da sind Sie froh, dass auf der Website des Geschäfts ein Kartenausschnitt zu sehen ist, der auch die nahe gelegenen Parkplätze zeigt. Vielleicht ist das Paket schwer zu tragen.
Vielleicht sind Sie aber auch bei dem Besuch der Website „getrackt" worden, ohne dass Sie es wussten und dem zugestimmt haben. Wenn Sie jetzt denken, den Cookie-Banner der Website hätten Sie gesehen und alle unnötigen Cookies abgelehnt, dann fühlen Sie sich womöglich nur auf der „sicheren Seite".

Kartendienste sind wie „Webseiten innerhalb der Webseiten"

Wenn zum Beispiel soziale Netzwerke, Videoplattformen oder eben Kartendienste (in Summe Drittdienste) in Webseiten eingebunden werden, bietet die eigentliche Webseite den Drittdiensten ein „Fenster" an, in dem zum Beispiel der Kartendienst Google Maps aktiv werden kann. Wird dann die Karte genutzt, verwendet man nicht nur die Website (zum Beispiel des Fachgeschäfts), sondern auch die eingebundene Webseite des Kartendienstes. Von dort können eigene Cookies und eigene Tracking-Versuche kommen, die auch separat kontrolliert werden müssen. Bevor die Kartendienste, Inhalte aus sozialen Netzwerken oder eingebundenen Videos in der jeweiligen Website

aktiviert und damit anzeigt werden, müssen die Besucherinnen und Besucher für das dann folgende Online-Tracking um eine informierte Einwilligung gebeten werden.

Datenschutzaufsicht berichtet von Mängeln

In der Praxis wird dies mitunter aber versäumt. So berichtete der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI), dass auf manchen Websites Tracking durch Drittdienste ohne Einwilligung der Nutzerinnen und Nutzer durchgeführt wird. Deshalb hatte der HmbBfDI eine große automatisierte Prüfaktion gestartet. Die meisten der insgesamt 1000 Websites, die nach dem Zufallsprinzip ausgewählt wurden, erfüllten die Datenschutzvorgaben. Bei 185 Hamburger Websites wurden aber auch Mängel festgestellt. Webdienste wurden dort unmittelbar bei Aufruf der Seite aktiviert, mit der Folge, dass Nutzende getrackt werden, ohne die dafür gesetzlich geforderte Einwilligung erteilt zu haben.

Oft ist es Betreibern von Websites weder bewusst, welche Drittdienste in ihren Angeboten eingebunden sind, noch welche datenschutzrechtlichen Anforderungen bei deren Einsatz erfüllt werden müssen, so die Datenschutzaufsicht. Als Beispiele für Drittdienste nennt die Aufsichtsbehörde unter anderem Google Maps, Facebook und YouTube.

Als Besucherin oder Besucher von Websites sollten Sie sich deshalb bewusst sein:

Wird der scheinbar hilfreiche Kartendienst auf der Website angezeigt, ohne Sie um eine Einwilligung zu bitten, könnte es sein, dass Sie in Ihren Online-Aktivitäten nachverfolgt werden, auch wenn Sie der Website selbst per Cookie-Banner mitgeteilt haben, dass Sie das nicht wollen.

Kennen Sie die Risiken durch den Fax-Versand? Machen Sie den Test!

Frage 1: Online-Tracking erfolgt nur mit den Cookies, die der Betreiber der Website auf Ihrem Endgerät speichern will. Stimmt das?

1. Nein, auch Dienste, die in die Website eingebunden wurden, könnten Online-Tracking ermöglichen.
2. Ja, deshalb ist es so wichtig, den Cookie-Banner der Website zu prüfen.

Lösung Frage 1: Die Antwort 1. ist richtig. Es ist zwar wichtig, den Cookie-Banner einer Website zu prüfen und dort die gewünschte Einstellung vorzunehmen. Aber Prüfungen von Datenschutzaufsichtsbehörden haben ergeben, dass Webseiten mitunter Dienste von Dritten einbinden, die selbst ein Online-Tracking vornehmen könnten. Leider fehlen dazu oftmals die Angaben in den Datenschutzerklärungen der betreffenden Websites.

Frage 2: Wenn ich im Cookie-Banner alle Cookies ablehne, sind auch die Tracking-Versuche durch Drittdienste auf den Websites gestoppt. Stimmt das?

1. Ja, denn man wählt ja aus, dass man alle Cookies ablehnt.
2. Nein, denn einige Websites kontrollieren das Tracking durch die Drittdienste wie Google Maps oder YouTube gar nicht. Werden Cookies abgelehnt, bedeutet das leider nicht automatisch, dass sich diese Entscheidung auch wie gewünscht auf die Drittdienste auswirkt.

Lösung Frage 2: Die Antwort 2. ist hier richtig. Werden zum Beispiel Kartendienste oder Videoplattformen in Webseiten eingebunden, können diese agieren wie Webseiten innerhalb von Webseiten. Es sind deshalb eigene Einstellung zu Cookies und anderen Tracking-Technologien notwendig. Leider fehlen manchmal aber die „Cookie-Banner“ für diese Drittdienste. Der Cookie-Banner der Haupt-Website reicht also nicht.